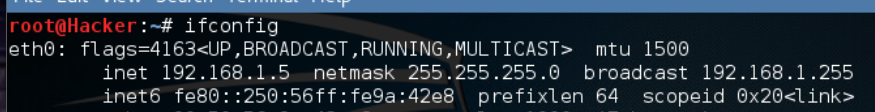
**CS547 – Secure Systems and Programs**

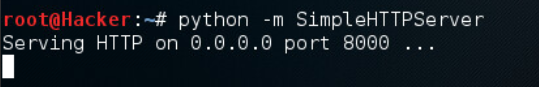
**Lab 6: Reflected XSS Mitigation and URL Encoding**

The requirements for this lab is to capture the screenshot of the below steps from given sections and submit in the word document.

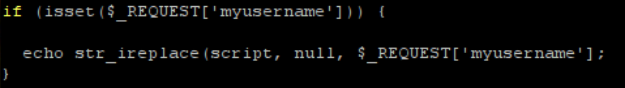
**Part 1**

**ENCODING**





**IMPLEMENTING A SECURITY CONTROL**



**VERIFYING THE CONTROL WORKS**

My kali host lost internet connection at the end of the virtual lab just like the last virtual lab. So I cant go to urbank.com or any other website anymore.

**PENTESTING ASSIGNMENT**

* **skip it**

**PART 2**

We use putty to SSH into the server. We execute the command to get the environment ready for the lab.

We figure out the ip address of the kali client which is 192168.1.5 . We then make this client start listening on port 8000.

We copy the malicious javascript and use it as our username to trick our victim to sending his cookie to our ip at the 8000 port.

We check our terminal and we cant see a new record. We go back to the browser and look at the source code to see why we didn’t get a new record. We can see that our ‘+’ character got interpreted as empty space.

We go back to the ubuntu host and connect to the server to edit the php file.

My kali host lost internet connection at the end of the virtual lab just like the last virtual lab. So I cant go to urbank.com or any other website anymore.